FAA National Software Conference, May 2002
Safety & Info Security Aspects of SW Assurance

The Leveraging of Safety and Information Security Engineering Principles: Establishing an Effective Level of Integrated Risk Management

By: Ronald Stroup
FAA Safety and Certification Lead

Warren Naylor
BAE SYSTEMS System Safety Manager

Michael LeBeau
BAE SYSTEMS System Safety Engineer

Goal: Enhanced Safety & Security While Maintaining Performance

- Establish sound safety and information security policy as the foundation for design
- Ensure safety and information security are an integral part of overall system design
  - Reduce risk to an acceptable level depending on criticality
  - Promote a common, coordinated, and comprehensive assessment process
  - Prevent conflicting requirements
  - Develop common mitigation techniques
- Ensure product team focuses on implementing requirements
- Identify trade-offs between reducing risk, increased costs, and decreased operational effectiveness

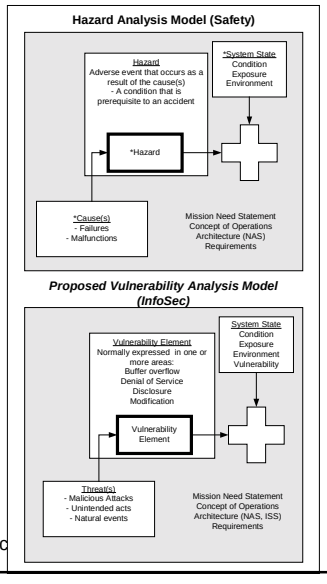
Mike Lebeau

Common Engineering Principles

- Establish a sound safety and security policy as the foundation for design
- Treat system safety and information security as an integral part of the overall system design
- All system operations represent some degree of risk
- Reduce risk to an acceptable level
- Keep hazards and vulnerabilities in the proper perspective
- Strive for simplicity
- Implement a technology refresh program
- Do not implement unnecessary risk mitigation mechanisms
- Identify and prevent common hazards and vulnerabilities

Analysis Models

- Hazard Analysis Model (Safety)
  - Causes
  - Hazards
  - System State
- Vulnerability Analysis Model (Information Security)
  - Threats
  - Vulnerabilities
  - System State



Risk Mitigation Strategy

- Hazard identification
- Hazard effect and risk level
- Requirements balance
- Requirements incorporation

Integrated Risk Index

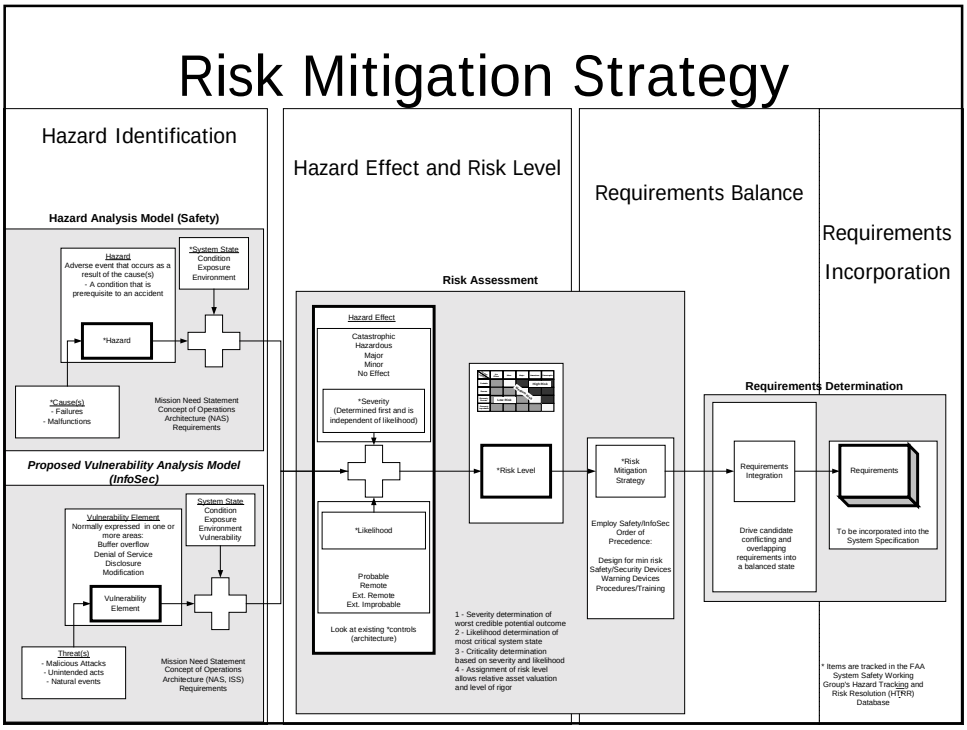
		Severity				
		No Effect	Minor	Major	Hazardous	Catastrophic
Likelihood of Occurrence	Probable					
	Improbable					
	Extremely Remote					
	Extremely Improbable					

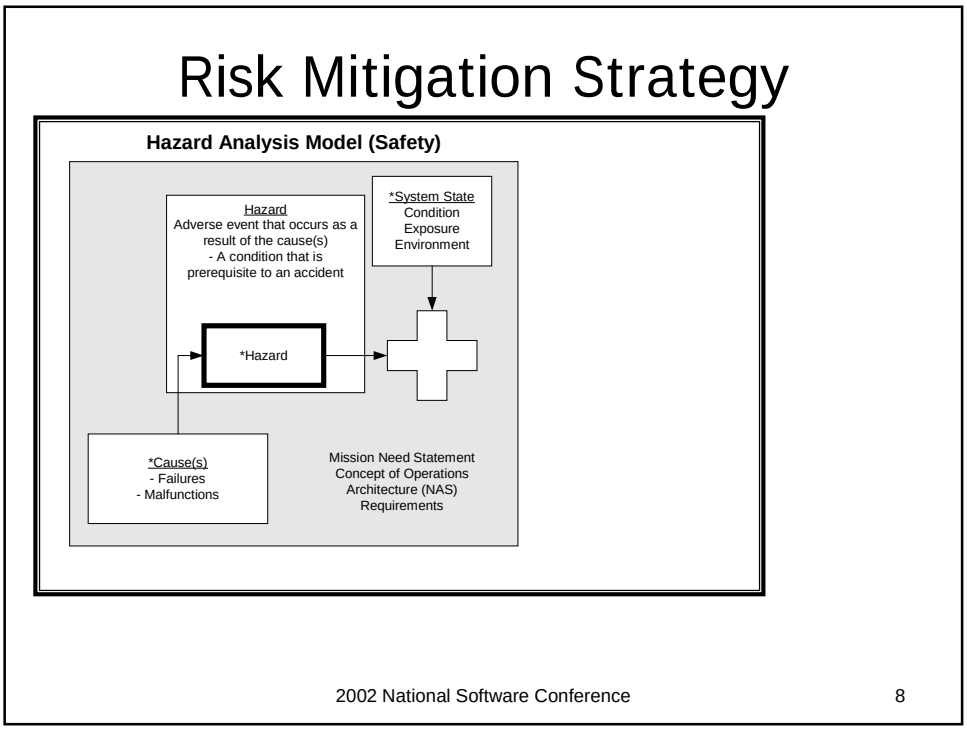
High

Medium

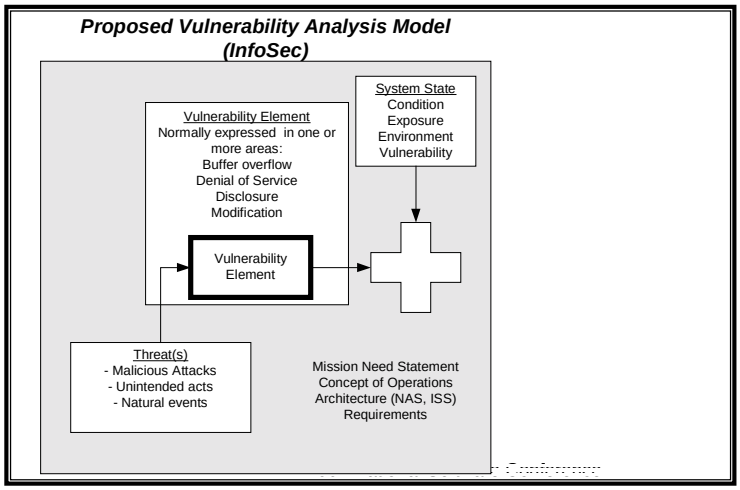
Low

FAA National Software Conference, May 2002
Safety & Info Security Aspects of SW Assurance



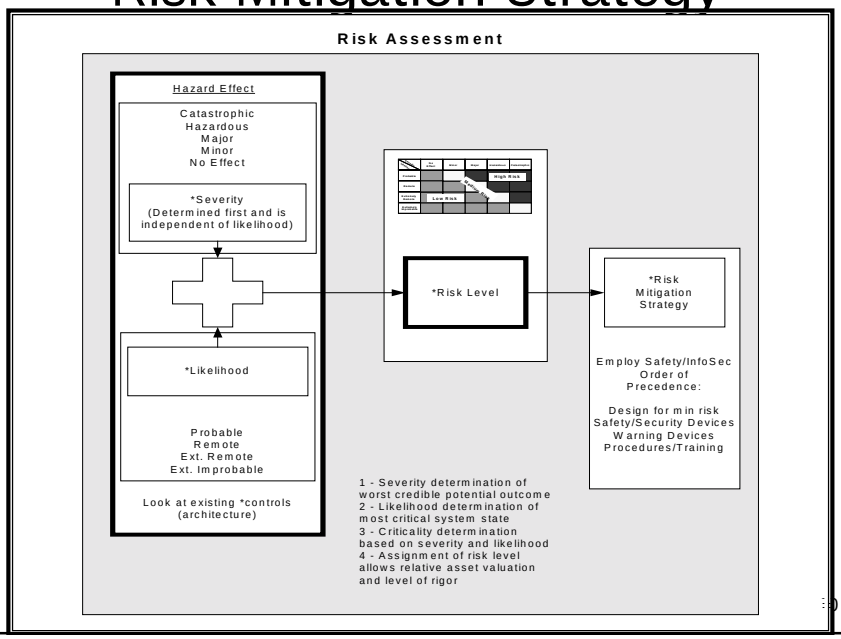


Risk Mitigation Strategy



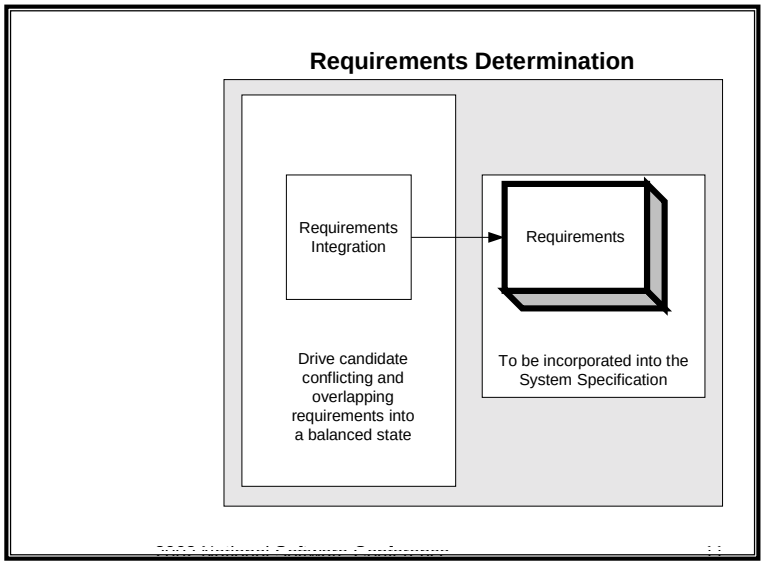
9

Risk Mitigation Strategy



10

Risk Mitigation Strategy



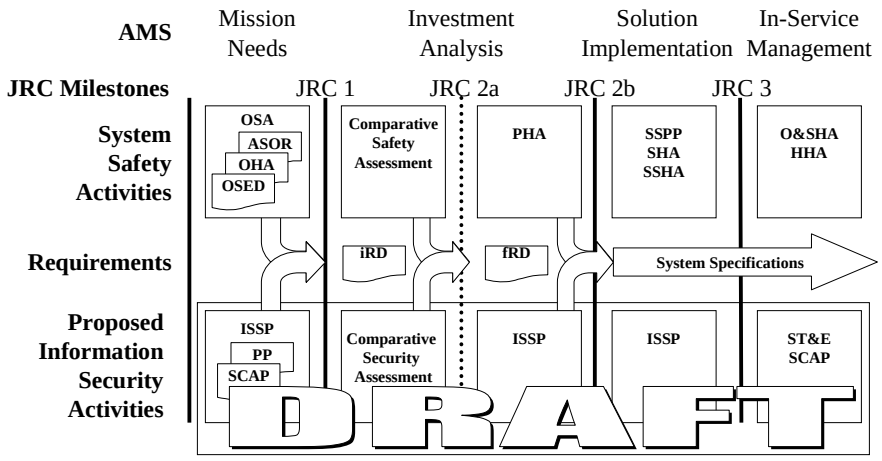
Roles of Risk Mitigation Objectives

- Risk mitigation services: confidentiality, integrity, availability, authentication, non-repudiation
- Resolves conflicting and/or overlapping risk mitigation requirements
- Reduces system design complexity and cost
- De-confliction of requirements occurs prior to system design activities

Mechanisms	Confidentiality	Integrity	Availability
Firewalls	X		
Checksum		X	
Encryption	X	X	
Watchdog Timer		X	X

2002 National Software Conference 12

Process Alignment



Summary

- Technical:
  - Reduced complexity in system design
  - Balanced set of risk mitigation requirements
- Programmatic:
  - Better aligned with system lifecycle
  - Simplified program management
- Economic:
  - More accurate program baseline
  - Increased probability of maintaining cost and schedule targets